UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, Plaintiff, v. DOES 1–18, et al., Defendants.	)	Civil Action No. 1:13cv139

REPORT AND RECOMMENDATION

This matter comes before the Court on Motion for Default Judgment by plaintiff Microsoft Corporation ("plaintiff" or "Microsoft") against defendant Dmitry Chupakhin ("defendant" or "Chupakhin"). (Dkt. 60.) After a representative for defendant failed to respond to plaintiff's Motion or to appear at the hearing on November 22, 2013, the undersigned Magistrate Judge took plaintiff's Motion under advisement.[1]

INTRODUCTION

I. Background

Plaintiff Microsoft, a Washington corporation, filed suit against defendant Dmitry Chupakhin, a resident of the Russian Federation, on January 31, 2013. (Compl. ¶¶ 1-3.) By way of

[1] The record before the Court includes the Complaint (Dkt. 1), plaintiff's Amended Complaint ("Am. Compl.") (Dkt. 50), plaintiff's Brief in Support of Microsoft's Request for Entry of Default (Dkt. 58) and supporting attachments thereto (Dkts. 58-1 through 58-11), the Motion for Default Judgment ("Mot. Def. J.") (Dkt. 60), and plaintiff's Memorandum in Support of Motion for Default Judgment ("Mem. Supp. Mot. Def. J.") (Dkt. 61).

its Amended Complaint of June 17, 2013, plaintiff clarified the defendants and issues pertinent to this matter. (Am. Compl. ¶¶ 1-5.) Plaintiff claims that defendant operated and controlled the Bamital computer botnet, which infected a large number of internet users' computers. (Id. at ¶ 4; Mot. Def. J. 1.) Defendant allegedly used various techniques to lure victims to websites where malicious botnet code was surreptitiously installed on their computers. (Am. Compl. ¶¶ 36-54; Mem. Supp. Mot. Def. J. 1.) Defendant was then able to make unauthorized changes to infected computers, bring them under his control, and force users' web browsers to websites of his choosing. (Id.) The code also created invisible browser instances that generated fraudulent clicks on advertisements and websites identified by defendant. (Id.) Defendant monetized these activities through the online advertising ecosystem, and caused injury to Microsoft, its customers, and the general public in a variety of ways. (Id.)

Plaintiff' brought claims based on (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 2701; (2) trademark infringement under the Lanham Act, 15 U.S.C. § 1115 *et seq*.; (3) false designation of origin under The Lanham Act, 15 U.S.C. § 1125(a); (4) trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c); (5) common law trespass to chattels; (6) unjust enrichment; and, (7) conversion. (Am. Compl. ¶ 1.) Plaintiff

now moves for the entry of default judgment and a permanent injunction against defendant that prohibits defendant from operating the Bamital botnet, and transfers ownership and control of the botnet domains and subdomains to Microsoft. (Mem. Supp. Mot. Def. J. 2.)

II. Jurisdiction and Venue

Rule 55 of the Federal Rules of Civil Procedure provides for the entry of default judgment when "a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend." The court must have both subject matter and personal jurisdiction over a defaulting party before it can render default judgment.

This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action involves claims brought pursuant to the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Electronic Communications Privacy Act, 18 U.S.C. § 2701, and the Lanham Act, 15 U.S.C. §§ 1114 & 1125. The Court also has subject matter jurisdiction under 28 U.S.C. § 1367 because this action includes claims for trespass to chattels, unjust enrichment, and conversion.

Virginia Code § 8.01-328.1(A)(1) provides that a Virginia court may exercise personal jurisdiction over any person in a matter related to that person's business transactions in the Commonwealth of Virginia. Defendant undertook the acts alleged

to cause harm through the ".com," ".net," and ".org" domain names located in this district, through IP addresses and users' computers located in this district, and harmed plaintiff, its customers, and others throughout this district. (Am. Compl. ¶ 22.) Therefore, jurisdiction over defendant is proper because of defendant's business transactions in the Commonwealth.

Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district for two reasons. First, a substantial part of the property involved in this action and events giving rise to plaintiff's claims occurred in this district. (Am. Compl. ¶ 23.) Second, in accordance with 28 U.S.C. § 1391(b), venue is proper in this district because a domain name is deemed to have its situs in the judicial district in which the domain name registry that registered or assigned the domain name is located. Here, the registries for the Bamital botnet domains, Verisign Naming Services and Verisign Global Registry Services (collectively "Verisign") and Public Interest Registry, are located in this district. (Id. at ¶¶ 10-11, 23.) Leaseweb, an internet service provider for the Bamital botnet IP addresses, is also located in this district. (Id. at ¶ 23.)

III. Service of Process

The Russian Federation no longer complies with formal requests for judicial assistance pursuant to the Hague Convention from the United States. Therefore, service of

process may be carried out by alternative methods that comport with the laws of the Russian Federation, the Federal Rules of Civil Procedure, and principles of Due Process. See, e.g., RSM Prod. Corp v. Fridman, No. 06-cv-11512, 2007 U.S. Dist. LEXIS 58194, at *5-6 (S.D.N.Y. Aug. 10, 2007) (approving service of process by non-treaty based means upon an individual in Russia, in view of suspension of Hague Convention processes). Plaintiff shows that it sufficiently served defendant, located in the Russian Federation, in multiple ways.

Plaintiff first served defendant with English and Russian translated copies of the Amended Complaint and Summons by international courier on July 8, 2013. (Dkt. 58-1 at ¶¶ 10-11.) Defendant signed for and received those documents at his address in the Russian Federation. (Id.; Dkts. 58-3, 58-4, 58-5, 58-6.) Plaintiff also served defendant with English and Russian translated copies of the Amended Complaint and Summons by registered delivery through the Russian Post on September 12, 2013. (Dkt. 58-7 at ¶ 2.) Those documents were received and signed for at defendant's address. (Id.) This latter method of service is authorized by the Code of Civil Procedure of the Russian Federation, Articles 113 and 115, which govern service of process in Russian courts. (Id.; Dkt. 58-11.) Service was therefore proper under Fed. R. Civ. P. 4(f)(2)(C)(i) and Fed. R. Civ. P. 4(f)(2)(A). See also Elrod v. Busch Entm't Corp., No.

4:09-cv-164, 2011 U.S. Dist. LEXIS 69459, at *6 (E.D. Va. June 1, 2011) (personal service on defendant in India sufficient where defendant provided signature acknowledging receipt pursuant to Fed. R. Civ. P. 4(f)(2)(C)(i)).

Plaintiff further demonstrated effective service on Dmitry Chupakhin by sending copies of the Amended Complaint, Summons, Russian translations, a link to all pleadings in this action, and the notice language approved by the Court in the temporary restraining order ("TRO") to defendant's email addresses on August 19, 2013, and August 23, 2013. (Dkt. 58-1 at ¶ 14; Dkt. 58-5.) Plaintiff also sent copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains. (Id. at ¶ 16.) Finally, beginning on February 7, 2013, plaintiff published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com. (Dkt 58-1 at ¶ 17.) This service by e-mail and internet publication to defendant Dmitry Chupakhin is authorized by Fed. R. Civ. P. 4(f)(3). See, e.g., Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1018 (9th Cir. 2002) ("If any method of communication is reasonably calculated to provide [defendant operating online] with notice, surely it is email—the method of

communication which [defendant] utilizes and prefers."); FMAC Loan Receivables v. Dagra, 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts readily use Rule 4(f)(3) to authorize international service through non-traditional means, including email).

Therefore, because plaintiff provided ample notice of this action through the aforementioned means, service of process was proper.

IV. Grounds for Default Judgment

Plaintiff filed this action on January 31, 2013. (Dkt. 1.) On that same date, plaintiff moved for and the Court granted a temporary restraining order and preliminary injunction, which allowed plaintiff to disable and seize the Bamital botnet's command and control servers' software. (Dkts. 3-9.) Plaintiff executed the TRO on February 7, 2013. (Dkt. 27.) On February 13, 2013, the Court issued a preliminary injunction authorizing plaintiff to disable the domains from which defendant operated and controlled the Bamital botnet during the pendency of this litigation. (Dkt. 38.)

On June 19, 2013, plaintiff filed the Amended Complaint naming Chupakhin as the defendant responsible for the alleged activities. (Dkt. 50.) On October 18, 2013, the Clerk of this Court entered default pursuant to plaintiff's Request for Entry of Default and Federal Rule of Civil Procedure 55. (Dkt. 59.)

Plaintiff filed its Motion for Default Judgment (Dkt. 60) and a Memorandum in Support of its Motion for Default Judgment (Dkt. 61) on October 24, 2013.

After defendant failed to appear at the November 22, 2013, hearing on plaintiff's Motion for Default Judgment, the undersigned took this matter under advisement. (Dkt. 65.) To date, no defendant has appeared or otherwise participated in these proceedings.

FINDINGS OF FACT

Upon a full review of the pleadings, the undersigned Magistrate Judge finds that plaintiff established the following facts.

Plaintiff Microsoft is a Washington corporation with its principal place of business in Redmond, Washington. (Am. Compl. ¶ 2.) Defendant Dmitry Chupakhin, also known as "Sergey Skorovod," is believed to reside in the Russian Federation. (Id. at ¶ 4.)

Microsoft supplies the Windows operating system, the Internet Explorer web browser, the Bing search engine, the Bing Ads advertising platform, and a variety of other software programs and services. (Id. at ¶ 24.) Microsoft has invested substantial resources in developing high-quality products and services, and has generated goodwill as a result of its branding and trade. (Id.) Microsoft possesses registered trademarks for

the Microsoft, Windows, Internet Explorer, and Bing marks, including trademark registration numbers 2872708, 2463526, 2277112, and 3883548. (Id.; Dkt. 50-4.)

Microsoft does business with companies that wish to advertise products online. (Id. at ¶ 26.) Microsoft allows advertisers to manage their advertising campaigns online through its Bing Ads platform. (Id. at ¶¶ 25-26.) For many of these advertisements, end-users may click on a link to view additional product information and take other actions. (Id. at ¶¶ 26-27.) These actions are tracked by advertisers, and monetized through the pay-per-click advertising system. (Id.)

The pay-per-click advertising system generates revenue for the publisher of the website where the click occurred by charging the initial advertiser for the number of hits generated by that advertisement. (Id. at ¶ 28.) These systems allow publishers to profit from the time, effort and money invested in developing websites, and allows advertisers to benefit by the placement of advertisements that are likely to attract interested end-users. (Id.)

Pay-per-click systems are susceptible to various fraudulent schemes. (Id. at ¶ 29.) For example, publishers may infect end-users' computers with malware that generates a large number of clicks for certain advertisements that, in turn, create high revenue for publishers through pay-per-click agreements. (Id.)

In other schemes, cybercriminals may generate large quantities of invalid clicks by redirecting innocent end-users' web browsers to specified websites or by deceiving the end-users into clicking on online advertisements. (Id. at ¶ 30.) This bad traffic can be sold and bought by parties online, as it can generate substantial payments from advertisers that are conned into paying for invalid clicks. (Id. at ¶ 31.)

Perpetrators of these fraudulent schemes often use botnets to increase their effect. (Id.) Botnets are large collections of computers that have been infected with common malware. (Id. at ¶ 33.) An individual computer is added to the botnet when the end-user inadvertently downloads malicious software, which allows the computer to be controlled by the botnet operator using a command and control computer. (Id. at ¶¶ 33-34.) The command and control computer allows the botnet operator to dictate certain actions on end-users' computers, such as sending bulk and unsolicited email, delivering malware to infect further computers, or carrying out fraud, computer intrusions, and other misconduct. (Id. at ¶ 35.)

Defendant Dmitry Chupakhin operates and controls the Bamital botnet from and through various internet domain names and subdomain names.[2] (Id. at ¶ 1.) Defendant uses fraudulent

[2] The Bamital botnet utilizes three groups of command and control servers. (Am. Compl. ¶ 42.) Plaintiff identified the specific

techniques to lure victims to websites from which malicious botnet code is installed on their computers. (Id. at ¶ 39.) Once infected, defendant directs Bamital-infected end-users' computers to engage in click-fraud either through hijacking web browsers or by instructing them to generate automated internet traffic. (Id. at ¶ 40.) The Bamital botnet also allows defendant to perform other illegal activity on infected end-users' computers, such as identity theft and cyber-attacks that render entire computer networks inoperable. (Id.) Most if not all owners of Bamital-infected computers are unaware that their machines are infected and operating as part of the Bamital botnet. (Id.)

The Bamital botnet causes harm to plaintiff and its customers in multiple ways. (Id. at ¶¶ 48-54.) The botnet malware is clandestinely installed onto computers without obtaining authorization or consent by Microsoft or end-users. (Id. at ¶ 48.) The botnet code creates invisible browser instances which, unbeknownst to users, generate fraudulent clicks and may deteriorate the performance of end-users'

---

domains hosting the main command and control domains in Appendix A to the Amended Complaint. (Dkt. 50-1.) Bamital's malware's module "a" servers, which are responsible for browser hijacking, are identified by their domains and IP addresses in Appendix B to the Amended Complaint. (Am. Compl. ¶ 44; Dkt. 50-2.) Bamital's module "c" servers, which can launch hidden instances of web browsers, are identified in Appendix C to the Amended Complaint by a listing of the domains hosting that module. (Am. Compl. ¶ 46; Dkt. 50-3.)

computers. (Id. at ¶ 50.) Similarly, the botnet may collect personal information, run software without end-users' consent, misuse the Windows operating system, and generate fake traffic that induces advertisers to pay publishers for fraudulent clicks and feigned activity. (Id. at ¶¶ 49-52.) These actions have caused many Microsoft customers to inadvertently attribute Microsoft as the source of these problems, thereby tarnishing the reputation of Microsoft's brand. (Id.)

EVALUATION OF PLAINTIFF'S COMPLAINT

Where a defendant has defaulted, the facts set forth in the plaintiff's complaint are deemed admitted. Before entering default judgment, however, the Court must evaluate the plaintiff's complaint to ensure that the complaint properly states a claim. GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 612 n.3 (E.D. Va. 2003). As such, it is appropriate to evaluate plaintiff's claim against the standards of Fed. R. Civ. P. 12(b)(6).

Plaintiff moves for the Court to grant default judgment and issue a permanent injunction against defendant Dmitry Chupakhin. (Mem. Supp. Mot. Def. J. at 1.) Plaintiff voluntarily dismissed its claims against defendant Marat Mazynskij on September 19, 2013. (Dkt. 56.) The grounds for default judgment are based on plaintiff's claims of (1) Computer Fraud and Abuse Act violations; (2) Electronic Communications Privacy Act

violations; (3) Lanham Act violations; (4) trespass to chattels/conversion; and, (5) unjust enrichment. (Mem. Supp. Mot. Def. J. 1.) Each claim is addressed in turn.

I. Computer Fraud and Abuse Act Violations

The Computer Fraud and Abuse Act ("CFAA") prohibits computer fraud effectuated on protected computers. 18 U.S.C. § 1030 *et seq*. The statute penalizes a party that

> intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C));
>
> intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C)); or,
>
> knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer (18 U.S.C. § 1030(a)(5)(A)).

Under the CFAA, a "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B).

The CFAA was designed to prevent the sort of unauthorized access and other fraudulent activity effectuated by malware and botnet activity. See, e.g., Global Policy Partners, LLC v.

Yessin, No. 1:09-cv-859, 2009 U.S. Dist. LEXIS 112472 (E.D. Va. Nov. 24, 2009) (accessing user's computer using credentials not belonging to defendant found actionable pursuant to the CFAA); Physicians Interactive v. Lathian Sys., Inc., No. 1:13-cv-1193, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. December 5, 2003) (CFAA violation where defendant hacked into user's computer and stole confidential information).

Here, plaintiff sufficiently pleads facts to show that defendant violated the CFAA. The Microsoft servers and end-users' computers are "protected computers" under the CFAA, because they are used in a manner that effects interstate or foreign commerce or communications within the United States. (Am. Compl. ¶¶ 55-60; Mem. Supp. Mot. Def. J. 9.) Defendant knowingly and intentionally accessed Microsoft's servers, Microsoft's proprietary operating system, Internet Explorer software, and Bing search engine functionality, as well as Microsoft's customers' computers. (Id.) Defendant burdened those computers by infecting them with the Bamital botnet malware, hijacking search engine browser sessions, forcing customers to visit unintended websites, and invisibly generating a large number of fraudulent clicks that defendant monetized through fraud upon the online advertising ecosystem. (Id.) Defendant effectuated these intrusions and harms without consent or authorization from plaintiff or its customers. (Id.)

Therefore, defendant violated the Computer Fraud & Abuse Act.

II. Electronic Communications Privacy Act Violations

The Electronic Communications Privacy Act ("ECPA") prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or "intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). Obtaining stored electronic information through the use of botnets, malware, and other malicious electronic entry violates this Act. See, e.g., Global Policy Partners, 2009 U.S. Dist. LEXIS 112472 at *8-13 (unauthorized access to emails deemed actionable under the ECPA); State Analysis, Inc. v. Am. Fin. Servs. Assoc., 621 F. Supp. 2d 309, 317-18 (E.D. Va. 2009) (unauthorized access of computer data supports basis for ECPA claims); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (unauthorized access of stored data on third-party communication service provider system violates the ECPA).

Plaintiff alleges a sufficient factual basis for the Court to find that defendant's actions violated the ECPA. Microsoft's search engine servers, Windows operating system, and Internet Explorer software are facilities through which electronic

communication services are provided. (Am. Compl. ¶¶ 61-65; Mem. Supp. Mot. Def. J. 10.) Defendant's Bamital botnet used computer codes to hijack internet browsers and search engines by intercepting communications to and from Microsoft servers, and forcing end-users to visit certain websites. (Id.) These actions were done without the end-users' consent, and allowed defendant to monetize end-users' forced activities. (Id.) Therefore, plaintiff showed that defendant violated the ECPA.

III. Lanham Act Violations

Plaintiff alleges that defendant committed three violations of the Lanham Act, 15 U.S.C. § 1051 *et seq*. Specifically, plaintiff claims that defendant is liable for (1) trademark infringement pursuant to 15 U.S.C. § 1114; (2) false designation of origin pursuant to 15 U.S.C. § 1125(a); and, (3) trademark dilution pursuant to 15 U.S.C. § 1125(c). (Am. Compl. ¶¶ 66-91.)

A. Trademark Infringement - Lanham Act 15 U.S.C. § 1114

The Lanham Act prohibits the use of a reproduction, counterfeit, copy, or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or to deceive. 15 U.S.C. § 1114(1). The statute specifically provides for relief against

> (1) Any person who shall, without the consent of the registrant—

> (a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or
>
> (b) reproduce, counterfeit, copy, or colorably imitate a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive.

(Id.) A defendant may be held liable for trademark infringement under this provision of the Lanham Act for unauthorized and improper use of a registered mark in connection with online advertising or other internet usage. See, e.g., Otels, Inc. v. Altun, No. 1:11-cv-604, 2012 U.S. Dist. LEXIS 114584 (E.D. Va. August 14, 2012) (unauthorized online use of registered mark deemed likely to cause confusion among consumers, constituting a violation of 15 U.S.C. § 1114(1)); Audi AG v. Shokan Coachworks, Inc., 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (finding 15 U.S.C. § 1114(1) trademark infringement where confusion was likely to result from unauthorized use of plaintiffs' name and images in connection with defendants' advertisements); Brookfield Commc'ns. v. W. Coast Entm't Corp., 174 F.3d 1036, 1066-67 (9th Cir. 1999) (Lanham Act trademark infringement for

various improprieties in connection with software and website codes).

Here, plaintiff sufficiently pleads facts to support a claim of trademark infringement under 15 U.S.C. § 1114(1). Plaintiff owns registered and famous trademarks, including Windows, Internet Explorer, and Bing. (Am. Compl. ¶ 24.) Defendant's Bamital botnet generated and used counterfeit copies of these marks in connection with his click-fraud scheme by distributing fake and manipulated versions of these marks. (Id. at ¶ 68; Mem. Supp. Mot. Def. J. 11.) Defendant used these counterfeits to deceive victims into believing that they were using legitimate versions of the software despite impaired functionality caused by the Bamital botnet malware. (Id.) This activity caused confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and the products promoted through the fake websites, resulting in harm to plaintiff. (Id. at ¶¶ 68-72; Mem. Supp. Mot. Def. J. 11.) Therefore, plaintiff shows that defendant's actions constituted trademark infringement under the Lanham Act.

B. False Designation of Origin - Lanham Act 15 U.S.C. § 1125(a)

The Lanham Act prohibits use of a trademark, any false designation of origin, false designation of fact, or misleading representation of fact which

is likely to cause confusion, or to cause mistake, or

> to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person

15 U.S.C. § 1125(a). Online communications and activities that bear misleading and fake information violate this provision of the Lanham Act. See e.g. America Online v. IMS, 24 F. Supp. 2d 548, 551-52 (E.D. Va. 1998) (spam email with fake sender addresses showing plaintiff's trademarks constituted false designation of origin); CJ Prods. LLC v. Snuggly Plushez LLC, 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (15 U.S.C. § 1125(a) violation for trademark infringement on website); Brookfield Commc'ns., 174 F.3d at 1066-67 (15 U.S.C. § 1125(a) violation for trademark infringement in software and website code).

Here, plaintiff shows that defendant's actions constituted false designations of origin under 15 U.S.C. § 1125(a). Defendant's Bamital botnet used misleading and counterfeit versions of plaintiff's protected trademarks to cause confusion as to Microsoft's affiliation with the botnet's conduct. (Am. Compl. ¶¶ 76-77; Mem. Supp. Mot. Def. J. 12.) These actions caused confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites, products, and services promoted through the fraudulent activities. (Id.) Therefore, defendant's actions violated 15 U.S.C. § 1125(a).

C. Trademark Dilution - Lanham Act 15 U.S.C. § 1125(c)

The Lanham Act provides that the owner of a famous mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury." 15 U.S.C. § 1125(c). Trademark dilution under this section of the Lanham Act involves copying and/or mimicking protected marks online. See e.g. America Online, 24 F. Supp. 2d at 552 (spam email with sender addresses that included plaintiff's trademarks violated 15 U.S.C. § 1125(c)).

Plaintiff's Amended Complaint contains a sufficient factual basis to find that defendant is liable for trademark dilution under the Lanham Act. The Bamital botnet generated counterfeit copies of plaintiff's protected marks for defendant's click-fraud scheme, and defendant used those marks to access end-users' computers. (Am. Compl. ¶¶ 84-86; Mem. Supp. Mot. Def. J. 13.) By doing so, defendant caused dilution of Microsoft's marks by improperly associating those marks with malicious conduct, actions, products, and services carried out or promoted by defendant through the Bamital botnet. (Id.) Therefore, defendant's actions constituted trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c).

IV. Trespass to Chattels and Conversion

A trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "the chattel is impaired as to its condition, quality, or value." American Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998); American Online, Inc v. IMS, 24 F. Supp. 2d at 550 (citing Vines v. Branch, 418 S.E. 2d 890, 894 (Va. 1992)). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." James River Mgmt. Co., Inc. v. Kehoe, No. 3:09-cv-387, 2009 U.S. Dist. LEXIS 107847, at *22-23 (E.D. Va. 2009). The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims. See, e.g., America Online, Inc. v. IMS, 24 F. Supp. 2d at 550 (senders of spam e-mail committed trespass when they "caused contact with [plaintiff's] computer network . . . [and] injured [plaintiff's] business goodwill and diminished the value of its possessory interest in its computer network").

Here, plaintiff alleges facts sufficient to show that defendant committed common law trespass to chattels. Through

the Bamital botnet, defendant accessed computers and servers associated with Microsoft's Internet Explorer, Bing, and Bing Ads without authorization. (Am. Compl. ¶¶ 92-97; Mem. Supp. Mot. Def. J. 13-14.) This unauthorized access allowed defendant to engage in click-fraud by directing web browser sessions and search engine results to websites of defendant's choice. (Am. Compl. ¶ 93; Mem. Supp. Mot. Def. J. 13.) These actions caused injury to Microsoft and its customers by lost time and money, and tarnished Microsoft's business goodwill. (Am. Compl. ¶¶ 95-97; Mem. Supp. Mot. Def. J. 13.) Therefore, defendant committed common law trespass to chattels.

Plaintiff also sufficiently shows that defendant committed conversion. Defendant, through the botnet, willfully interfered with and converted Microsoft's property in a way that allowed defendant to control Microsoft software, servers, and search engines. (Am. Compl. ¶¶ 108-111; Mem. Supp. Mot. Def. J. 24.) Microsoft was deprived of the full use and possession of its property because of this unlawful trespass. (Id.) Therefore, defendant's actions support the elements necessary to prove conversion.

V. Unjust Enrichment

A plaintiff proves a claim for unjust enrichment by showing (1) plaintiff's conferring of a benefit on the defendant; (2) defendant's knowledge of the conferring of the benefit; and, (3)

defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." Nossen v. Hoy, 750 F. Supp. 740, 744-45 (E.D. Va. 1990).

Here, plaintiff shows all elements of this claim. Without authorization, defendant used Microsoft's servers, networks, Windows operating system, Internet Explorer, and Bing search engine to operate and propagate the Bamital botnet click-fraud scheme. (Am. Compl. ¶¶ 98-107; Mem. Supp. Mot. Def. J. 14.) Defendant did this by improperly installing the malware onto end-users' computers, which allowed him to hijack web browsers and search engines and direct fraudulent web traffic to specified websites. (Id.) Defendant profited from this activity, and it would be inequitable for defendant to retain the benefits from this unlawful scheme. (Id.) Therefore, the Amended Complaint supports a claim of unjust enrichment.

REQUESTED RELIEF

Plaintiff requests that the Court (1) grant default judgment against defendant Dmitry Chupakhin; (2) enter a permanent injunction prohibiting Chupakhin from engaging in the conduct underlying this case; and, (3) direct that the ownership and control of the botnet domains and subdomains at issue be transferred to Microsoft. For the reasons articulated above, the undersigned recommends that the Court grant this relief.

RECOMMENDATION

For the reasons outlined above, the undersigned recommends that default judgment be entered in favor of plaintiff Microsoft Corporation and against defendant Dmitry Chupakhin, and that the Court grant the following relief:

A. Defendant Dmitry Chupakhin, his representatives, and persons who are in active concert or participation with him are permanently enjoined from: intentionally accessing and sending malicious software to Microsoft's Windows operating system and the protected computers, operating systems and Internet Explorer and Bing software and search functionality, of Microsoft's customers, without authorization, in order to infect those computers and software and make them part of the botnet; sending malicious software to configure, deploy and operate a botnet; creating or using software or the Bamital botnet or carrying out any other activities that falsely indicate association with or approval of Microsoft; infringing Microsoft's Microsoft, Windows, Internet Explorer, or Bing trademarks; stealing information, computing resources or property from Microsoft or Microsoft's customers, or undertaking any similar activity that inflicts harm on Microsoft, its customers, or the public.

B. Defendant Dmitry Chupakhin, his representatives and persons who are in active concert or participation with him are permanently restrained and enjoined from configuring, deploying,

operating or otherwise participating in or facilitating the Bamital botnet described in the Amended Complaint, including but not limited to the command and control software hosted at and operating through the domains, subdomains and IP addresses set forth in the Amended Complaint and through any other component or element of the botnet in any location.

C. Defendant Dmitry Chupakhin, his representatives and persons who are in active concert or participation with him are permanently restrained and enjoined from using the trademarks "Microsoft," "Windows," "Internet Explorer," and "Bing," and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that defendant's products or services come from or are somehow sponsored by or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft or Microsoft's customers, or passing off goods or services as Microsoft's.

D. Defendant Dmitry Chupakhin, his representatives and persons who are in active concert or participation with him are permanently restrained and enjoined from infringing Microsoft's registered trademarks, Registration No. 2872708, 2463526, 2277112 and 388354.

E. Defendant Dmitry Chupakhin, his representatives and persons who are in active concert or participation with him are

permanently restrained and enjoined from using in connection with defendant's activities any false or deceptive designation, representation or description of defendant's or his representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give defendant an unfair competitive advantage or result in deception of consumers.

F. Defendant Dmitry Chupakhin shall forfeit control of the domains and subdomains identified in Appendix A to plaintiff's proposed order (Dkt. 62-1).

G. Pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries and domain registrars of the Bamital botnet domains and third-party subdomain providers responsible for the subdomains identified in Appendix A to plaintiff's proposed order (Dkt. 62-1) (collectively the "Domain and Subdomain Providers") shall implement the provisions of this Order in the following fashion:

1. Transfer the domains and subdomains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains and subdomains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor of other such registrar and account details specified by Microsoft. Subdomains should be transferred to subdomain

accounts under control of Microsoft, at the relevant subdomain provider.

2. The WHOIS or equivalent subdomain registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

3. The domains and subdomains shall be made active and shall resolve in the manner set forth in this order, or as otherwise be specified by Microsoft, upon its taking control of the domains and subdomains.

4. The domains and subdomains shall be assigned the authoritative name servers ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or such other name servers or IP addresses specified by Microsoft, and the Domain and Subdomain Providers shall take other

reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that defendant cannot use them to control the botnet.

5. The domains and subdomains shall remain active and continue to resolve in the manner set forth in this Order.

6. The Domain and Subdomain Providers shall prevent transfer or modification of the domains and subdomains by defendant and shall prevent transfer or control of the domains and subdomains to the account of any party other than Microsoft.

7. The Domain and Subdomain Providers shall take all steps required to propagate to the foregoing changes through the DNS, including domain registrars and/or subdomain services.

8. Non-U.S. Domain and Subdomain Providers are respectfully requested, but are not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the internet, to protect end-user victims of the Bamital botnet in all countries, to advance the public interest and to protect Microsoft and its customers from the Bamital botnet.

9. Third-party The Internet Corporation for Assigned

Names and Numbers ("ICANN"), 12025 Waterfront Dr., Suite 300, Los Angeles, California, 90094, is respectfully requested, but is not ordered, to use its best efforts to assist and facilitate the transfer of U.S.-based domains set forth in Appendix A to plaintiff's proposed order (Dkt. 62-1), to Microsoft.

NOTICE

The parties are advised that objections to this Report and Recommendation, pursuant to 28 U.S.C. § 636 and Rule 72(b) of the Federal Rules of Civil Procedure, must be filed within fourteen (14) days of its service. Failure to object to this Report and Recommendation waives appellate review of any judgment based on it.

The Clerk is directed to send a copy of this Report and Recommendation to all counsel of record and to defendant at the following address:

Dmitry Chupakhin
Barbyusa St., Bldg. 124, Apt. 24
Chelyabinsk 454078
Russian Federation

/s/
THERESA CARROLL BUCHANAN
UNITED STATES MAGISTRATE JUDGE

January 6, 2014
Alexandria, Virginia